

WHAT IS CLAIMED:

1 1. A system comprising:
2 a central processing unit operating in response to a
3 set of instructions for processing information;
4 an interface for providing access to selected circuitry
5 forming a part of said system on a chip by an external
6 device; and
7 a set of non-volatile programmable security elements
8 for selectively enabling and disabling the operation of said
9 interface to provide a private environment for processing
10 said information.

1 2. The system of Claim 1 wherein said interface comprises
2 a JTAG port.

1 3. The system of Claim 1 wherein said interface comprises
2 an in-circuit emulation port.

1 4. The system of Claim 1 wherein said interface comprises
2 a port allowing said external device to observe an internal
3 state of said integrated circuit.

1 5. The system of Claim 1 and further comprising boot
2 memory for storing security initialization code, said
3 security initialization code selectively enabled by
4 programming said set of programmable elements.

1 6. The system of Claim 5 and further comprising boot
2 memory for storing security initialization code, said
3 security initialization code selectively enabled by
4 programming said set of programmable elements.

0546581-00100

1 7. The system of Claim 1 and further comprising a cache
2 associated with said central processing unit, said cache
3 including a selected number of lockable entries for storing
4 secure information.

1 8. The system of Claim 1 and further comprising a
2 translation look aside buffer, with said CPU, said
3 translation look aside buffer including a selected number of
4 lockable entries for storing addresses to secure information
5 in memory

1 9. The system of Claim 1 and further comprising on-chip
2 random access memory including a selected amount of memory
3 space for storing address translation tables.

1 10. The system of Claim 1 wherein said set of programmable
2 elements comprises a set of fuses.

1 11. The system of Claim 1 wherein said set of programmable
2 elements comprise a set of bond options.

1 12. The system of Claim 1 wherein said set of programmable
2 elements comprises a set of antifuses.

1 13. The system of Claim 1 wherein said set of programmable
2 elements comprises a set of read-only memory cells.

1 14. The system of Claim 1 wherein said set of programmable
2 elements comprises a set of write-once memory cells.

1 15. The system of Claim 1 wherein said set of programmable
2 elements comprises a set of FLASH memory cells.

[illegible]

operating the system in a secure environment in response to the called security procedure when the called security procedure is valid.

THE UNIVERSITY OF CHICAGO

enabling the debug circuitry and
executing boot code pointed-to by the vector.

changing a program counter to the vector such that a fetch of an instruction changing the program counter is completed prior to completion of said step of remapping.

[illegible]

1 19. The method of Claim 18 wherein said vector comprises a
2 CPU reset vector.

20. The method of Claim 16 wherein execution of the security code in boot memory determines that the called security procedure is invalid and said method further comprises the steps of:

```

5      remapping the vector to the boot memory to a location
6      storing second selected security code, the second security
7      code calling a second security procedure;

```

```

8         executing the second selected security code in boot
9         memory to determine if the second security procedure is
0         valid; and

```

1 operating the system on a chip in a secure environment
2 in response to the second security procedure when the second
3 security procedure is valid.

21. The method of Claim 16 wherein said step of executing the security code in boot memory to determine whether the called security procedure is valid comprises the substep of searching for the called security procedure in external memory coupled to the system on a chip.

1 22. The method of Claim 16 and further comprising the step
2 of executing default boot code when the called security
3 procedure is invalid.

23. The method of Claim 16 wherein said step of determining
if a security procedure is called for during system
initialization comprises the substep of reading the state of
a set of programmable elements.

Q U E S T I O N

1 24. The method of Claim 23 wherein said substep of reading
2 is performed by logic gates.

1 25. The method of Claim 23 wherein said substep of reading
2 is performed by a central processing unit

0049581-020400

26. A method of preventing access and observation of encached information comprising the steps of:

- generating private information to be encached;
- storing the private information in memory;
- updating a translation look aside buffer with descriptors to locations in memory containing the private information;
- forcing a cache miss to a selected location in cache to be loaded with a selected portion of the private information;
- retrieving the selected portion of the private information from memory using a corresponding descriptor from the translation look aside buffer;
- loading the retrieved portion of the private information into the selected location in cache; and
- locking the selected portion of the private information in the selected location in cache.

27. The method of Claim 26 and further comprising the step of locking the descriptor corresponding to the selected portion of the private information in the translation look aside buffer.

28. The method of Claim 26 wherein said selected location in cache is associated with a replacement counter base and said step of locking comprises the substep of resetting the replacement counter base to a value higher than the replacement counter base associated with the selected location in cache.

29. The method of Claim 26 wherein said step of updating the translation look aside buffer comprises the substeps of:

- setting up a translation table including entries for generating the descriptors to memory locations storing the private information;
- updating a replacement counter to point to a current translation look aside buffer entry to be filled;
- forcing a miss to the current translation look aside buffer entry;
- performing a table walk through the translation table to generate a descriptor associated with private information in memory; and
- loading the descriptor obtained from the table walk in the current translation look aside buffer entry.

30. The method of Claim 26 wherein said step of loading the selected portion of the decoded information in cache comprises the step of loading a cache line in instruction cache.

31. The method of Claim 26 wherein said step of loading the selected portion of the private information in cache comprises the step of loading a cache line in data cache.

32. The method of Claim 26 wherein said step of setting up a translation table comprises the step of setting up an emulated translation table.

1. **Introduction**
 2. **Background**
 3. **Methodology**
 4. **Results**
 5. **Discussion**
 6. **Conclusion**
 7. **References**
 8. **Appendix**
 9. **Notes**
 10. **References**
 11. **Appendix**
 12. **Notes**
 13. **References**
 14. **Appendix**
 15. **Notes**
 16. **References**
 17. **Appendix**
 18. **Notes**
 19. **References**
 20. **Appendix**
 21. **Notes**
 22. **References**
 23. **Appendix**
 24. **Notes**
 25. **References**
 26. **Appendix**
 27. **Notes**
 28. **References**
 29. **Appendix**
 30. **Notes**
 31. **References**
 32. **Appendix**
 33. **Notes**
 34. **References**
 35. **Appendix**
 36. **Notes**
 37. **References**
 38. **Appendix**
 39. **Notes**
 40. **References**
 41. **Appendix**
 42. **Notes**
 43. **References**
 44. **Appendix**
 45. **Notes**
 46. **References**
 47. **Appendix**
 48. **Notes**
 49. **References**
 50. **Appendix**
 51. **Notes**
 52. **References**
 53. **Appendix**
 54. **Notes**
 55. **References**
 56. **Appendix**
 57. **Notes**
 58. **References**
 59. **Appendix**
 60. **Notes**
 61. **References**
 62. **Appendix**
 63. **Notes**
 64. **References**
 65. **Appendix**
 66. **Notes**
 67. **References**
 68. **Appendix**
 69. **Notes**
 70. **References**
 71. **Appendix**
 72. **Notes**
 73. **References**
 74. **Appendix**
 75. **Notes**
 76. **References**
 77. **Appendix**
 78. **Notes**
 79. **References**
 80. **Appendix**
 81. **Notes**
 82. **References**
 83. **Appendix**
 84. **Notes**
 85. **References**
 86. **Appendix**
 87. **Notes**
 88. **References**
 89. **Appendix**
 90. **Notes**
 91. **References**
 92. **Appendix**
 93. **Notes**
 94. **References**
 95. **Appendix**
 96. **Notes**
 97. **References**
 98. **Appendix**
 99. **Notes**
 100. **References**

1 33. A method of synthesizing translation tables comprising
2 the steps of:

3 setting up at least one register for storing
4 information controlling access to a plurality of memory
5 spaces;

6 generating a virtual address including a pointer to
7 selected information in the at least one register
8 controlling access to a selected one of the memory spaces;

9 accessing said selected information at said pointer
10 from the at least one register; and

11 generating a physical address to the selected one of
12 the memory spaces from the information accessed from the at
13 least one register.

1 34. The method of Claim 33 wherein the selected information
2 comprises access permissions.

1 35. The method of Claim 33 wherein the selected information
2 comprises cacheability and bufferability bits.

1 36. The method Claim 33 wherein the at least one register
2 comprises a first register for storing access permissions
3 associated with each of the memory spaces, a second
4 register for storing a cacheability bit associated with each
5 of the memory spaces and a third register for storing a
6 bufferability bit associated with each of the memory spaces.

001020 ET856460

37. The method of Claim 33 wherein the selected information accessed from the at least one register comprises a base address to at least one second level register controlling access to a selected part of a selected one of the memory spaces and said step of generating a physical address comprises the substeps of:

accessing selected information in the at least one second level register using the base address and a table index from the virtual address; and

generating the physical address from the selected information accessed from the at least one second level register and page index bits from the virtual address.

38. The method of Claim 33 wherein said information includes for each of the memory spaces a pair of access permission bits, a bufferability bit and a cacheability bit.

39. A method of performing an emulated translation table walk comprising the steps of:

- emulating a translation register including a plurality of entries populated with descriptors;
- emulating an index register storing indices associated with the entries of the emulated translation register;
- pointing to the emulated translation register with a translation base pointer;
- generating an address including index bits to the emulated translation register;
- comparing the index bits from the address with the indices stored in the index register; and
- selectively accessing a corresponding descriptor in the translation table in response to said step of comparing.

1 40. The method of Claim 39 wherein said step of generating
2 an address comprises the step of generating a virtual
3 address forcing a miss to an associated cache.

41. The method of Claim 39 wherein the descriptors comprise selected physical address bits and access permissions and said method further comprises the steps of:

- determining from the permissions from the descriptor selectively accessed from the emulated translation table whether a corresponding access to memory is allowed; and
- if the access is allowed, generating a physical address to a location in memory using the physical address bits from the accessed descriptor.

in response to said step of comparing, selectively accessing a second level descriptor from the corresponding entry in the second level translation table.

if the access is allowed, generating a physical address to a location in memory using the second level physical address bits from the accessed second level descriptor.

2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 2494 2495 2496 2497 2498 2499 2500 2501 2502 2503 2504 2505 2506 2507 2508 2509 2510 2511 2512 2513 2514 2515 2516 2517 2518 2519 2520 2521 2522 2523 2524 2525 2526 2527 2528 2529 2530 2531 2532 2533 2534 2535 2536 2537 2538 2539 2540 2541 2542 2543 2544 2545 2546 2547 2548 2549 2550 2551 2552 2553 2554 2555 2556 2557 2558 2559 2560 2561 2562 2563 2564 2565 2566 2567 2568 2569 2570 2571 2572 2573 2574 2575 2576 2577 2578 2579 2580 2581 2582 2583 2584 2585 2586 2587 2588 2589 2590 2591 2592 2593 2594 2595 2596 2597 2598 2599 2600 2601 2602 2603 2604 2605 2606 2607 2608 2609 2610 2611 2612 2613 2614 2615 2616 2617 2618 2619 2620 2621 2622 2623 2624 2625 2626 2627 2628 2629 2630 2631 2632 2633 2634 2635 2636 2637 2638 2639 2640 2641 2642 2643 2644 2645 2646 2647 2648 2649 2650 2651 2652 2653 2654 2655 2656 2657 2658 2659 2660 2661 2662 2663 2664 2665 2666 2667 2668 2669 2670 2671 2672 2673 2674 2675 2676 2677 2678 2679 2680 2681 2682 2683 2684 2685 2686 2687 2688 2689 2690 2691 2692 2693 2694 2695 2696 2697 2698 2699 2700 2701 2702 2703 2704 2705 2706 2707 2708 2709 2710 2711 2712 2713 2714 2715 2716 2717 2718 2719 2720 2721 2722 2723 2724 2725 2726 2727 2728 2729 2730 2731 2732 2733 2734 2735 2736 2737 2738 2739 2740 2741 2742 2743 2744 2745 2746 2747 2748 2749 2750 2751 2752 2753 2754 2755 2756 2757 2758 2759 2760 2761 2762 2763 2764 2765 2766 2767 2768 2769 2770 2771 2772 2773 2774 2775 2776 2777 2778 2779 2780 2781 2782 2783 2784 2785 2786 2787 2788 2789 2790 2791 2792 2793 2794 2795 2796 2797 2798 2799 2800 2801 2802 2803 2804 2805 2806 2807 2808 2809 2810 2811 2812 2813 2814 2815 2816 2817 2

- 1 44. A system comprising:
2 a central processing unit operating in response to a
3 set of instructions for processing information;
4 an interface for providing access to selected circuitry
5 forming a part of said system on a chip by an external
6 device; and
7 a set of programmable security elements for selectively
8 enabling and disabling the operation of said interface to
9 provide a private environment for processing said
10 information.
- 1 45. The system of Claim 44 wherein said central processing
2 unit, said interface, and said security elements are
3 fabricated on a single integrated circuit chip.
- 1 46. The system of Claim 45 wherein said integrated circuit
2 chip further includes on-chip read-only memory.
- 1 47. The system of Claim 45 wherein said integrated circuit
2 chip further includes on-chip random access memory.
- 1 48. The system of Claim 44 and further comprising memory
2 storing private code for initializing private operation of
3 said system.
- 1 49. The system of Claim 44 wherein said system forms a
2 portion of a hand-held personal appliance.
- 1 50. The system of Claim 49 wherein said hand-held appliance
2 comprises and audio decoder.

1 51. A hand-held audio decoder comprising:
2 a central processing unit operating in response to a
3 set of instructions for decoding a stream of encoded digital
4 audio data;
5 memory for storing said set of instructions; and
6 digital to analog converter circuitry for generating
7 audio from said decoded stream of digital audio data.

1 52. The audio decoder of Claim 51 wherein said central
2 processing unit comprises an advanced risk machine.

1 53. The audio decoder of Claim 51 wherein said stream of
2 encoded digital data comprises a stream of MPEGx, Layer 3
3 encoded audio data.

1 54. The audio decoder of Claim 51 wherein said stream of
2 encoded digital data comprises a stream of ACC encoded
3 digital data.

1 55. The audio decoder of Claim 51 wherein said stream of
2 encoded digital data comprises a stream of MS Audio encoded
3 digital data.

1 56. The audio decoder of Claim 51 wherein said decoder is
2 capable of operating correctly from one AA battery for a
3 period of at least one hour.

57. A method of synthesized address translation comprising the steps of:

setting up at least one global register having a plurality of entries each for storing access control bits for a corresponding region of memory each comprising a plurality of locations having common access characteristics; and

setting up an individual register for storing a descriptor corresponding to a region of memory having differing access characteristics;

generating an address including an index;

in response to a first state of the index, accessing said descriptor from the individual register; and

in response to a second state of the index, performing the substeps of:

accessing the access control bits from a selected one of the global registers pointed-to by said index; and

generating a descriptor by merging the access control bits accessed from the selected one of the global registers with selected bits of said address.

58. The method of Claim 57 and further comprising the steps of:

```

    setting up a constant register for storing a constant;
and

```

in response to a third state of the index, accessing a constant from said constant register.

59. The method of Claim 58 wherein the constant register comprises hardwired gates.

1 60. The method of Claim 57 wherein the access control bits
2 comprise access permission bits, cacheability bits and
3 bufferability bits.

61. The method of Claim 57 wherein said at least one register comprises a first register having a plurality of entries each for storing access permission bits for a corresponding one of the regions, a second register having a plurality of entries each for storing a cacheability bit for a corresponding one of the regions and a third register having a plurality of entries each for storing a bufferability bit for a corresponding one of the regions.

001020"ET.85450

1 62. The method of Claim 57 wherein said descriptor
2 comprises first level descriptor including an second level
3 index, the method further comprising the steps of:
4 setting up at least one second level global register
5 having a plurality of entries each for storing access
6 control bits for a corresponding region of memory comprising
7 a plurality of locations having common access
8 characteristics; and
9 setting up a second level individual register for
10 storing a descriptor corresponding to a region of memory
11 having differing access characteristics;
12 in response to a first state of the second level index,
13 accessing the descriptor from the second level individual
14 register; and
15 in response to a second state of the second level
16 index, performing the substeps of:
17 accessing said access control bits from a selected
18 one of the second level global registers pointed-to by
19 said second level index; and
20 generating a second descriptor by merging the
21 access control bits accessed from the selected one of
22 the second level global registers with selected bits of
23 the address.

1 63. The method of Claim 62 and further comprising the
2 steps of:
3 setting up a second level constant register for storing
4 a second level constant; and
5 in response to a third state of the second level index,
6 accessing a second level constant from the second level
7 constant register.

ATTORNEY DOCKET NO.
_____-CS

PATENT

69

1 64. The method of Claim 58 wherein the second constant
2 register comprises hardwired gates.

1 65. The method of Claim 57 wherein the access control bits
2 comprise access permission bits, cacheability bits and
3 bufferability bits.

00495813 020100
00495813 020100